Monthly Cyber Security Tips Newsletter

September is "Disaster Preparedness Month." It's important to consider how we safeguard our information in the event of a natural disaster, man-made event, or even a system failure. This newsletter will discuss some steps you can take to secure your critical information and some best practices to make information security part of daily life.

What are some steps to safeguard physical forms of information?

Store all important documents in a secure and preferably fireproof, waterproof and portable container, as well as maintain a copy at an off-site location. Below is a list developed by the Federal Emergency Management Agency (FEMA) of important documents:

- Insurance policies, wills, contracts, deeds, stocks and bonds
- Photo IDs, passports, social security cards, immunization records
- Bank account numbers
- Credit card account numbers and companies
- Inventory of valuable household goods, important telephone numbers
- Family records (birth, marriage, death certificates)
- Photocopies of credit and identification cards

What about your digital information?

While the above items of information are maintained in a physical form, what about other important information stored in a digital form? This includes items such as any family photos, electronic billing and account information you maintain on your computer, list of contact information for family and friends, and any important projects you are working on your computer (such as family budgets, retirement planning information, construction plans, and other items that are difficult to rebuild or replace). You may be saving these pieces of information to your computer's hard drive, but if there is a flood or a hard drive failure this information may be lost forever. It is important to back up this same information, however you can choose different methods. Some methods include:

- Flash drives and portable hard drives represent a way to back up important information on smaller and more portable devices. These can be stored in your fire proof, waterproof and portable container or at a separate location (safe deposit box, etc.).
- You may consider using an email or online service to store some key documents.
- Consider backing up your phone as well. Most major phone providers and email services offer free or low cost contact backup services.

How to ensure your information is always protected?

It's important to make saving and storing your information a regular habit. Keep in mind that you may not be able to store everything, but make sure you save critical information with regularity. Below are some tips for making sure you are keeping your information protected in the event of a disaster:

Physical forms:

- When you change your insurance policy or update your identification, make a copy and place it in your emergency storage that day.
- Twice a year inventory your emergency storage and remove out-of-date or non-relevant information and add updated information.
- Once a year, check that all documents at off-site storage are up-to-date.

Digital forms:

- Save all files to your external storage (or online service) on a regular basis.
- Back up your hard drive frequently (daily, weekly, or monthly).
- Annually, review all files on external storage; remove ones that are no longer needed.

Resources for more information:

Ready America:

www.ready.gov/america/index.html

FEMA: Assemble a Disaster Supplies Kit:

www.fema.gov/plan/prepare/supplykit.shtm

Financial Planning, A Guide for Disaster Preparedness: Protecting Your Records

www.redcross.org/preparedness/FinRecovery/FinPlan/records.html#homesafe

For more monthly cyber security newsletter tips visit:

www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. **Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.**

Brought to you by: